



Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

HOLIDAY FRAUD SURGE

SUMMARY

During the holiday season, financial institutions tend to see a surge in fraud as scammers exploit increased online shopping, higher volumes of financial activity, especially cash transfers, and evolving cybercrime tactics, leading to more scams such as phishing, fake account-notification messages, and non-delivery fraud.

FACTORS CONTRIBUTING TO THE INCREASE

- **Higher transaction volume:** The sheer increase in online and in-store purchases creates more opportunities for fraudsters to operate undetected.
- **Stretched fraud detection teams:** Increased activity can overwhelm internal fraud detection systems, making it harder to spot suspicious behavior.
- **Behavioral shifts:** Consumer spending patterns change during the holidays with gift-giving and travel, which can complicate traditional fraud detection models that rely on predictable spending habits.
- **Increased digital payments:** The rise of online shopping leads to a spike in card-not-present attacks, phishing, and account takeovers.
- **Check fraud:** There is a surge in mail and financial transactions during the holidays, which creates a perfect environment for check theft and forgery.
- **First-party fraud:** This occurs when customers exploit return/refund policies for financial gain. These schemes include disputing legitimate charges, falsely reporting lost or stolen deliveries, and making purchases with no intention of paying.
- **Phishing, vishing, and smishing:** Scammers send fake emails, phone calls, or texts impersonating legitimate financial institutions, retailers, or shipping companies to steal sensitive information.
- **P2P (peer-to-peer) payment scams:** Scammers impersonate friends, family members, or banks to trick victims into sending them money through apps like Zelle, Venmo, or PayPal.

MITIGATING STEPS

- **Educate accountholders:** Financial institutions should educate accountholders on best practices, such as verifying sources, protecting personal information, and recognizing scam red flags.
- **Enhance internal systems:** Consider implementing behavioral analytics, biometrics, advanced AI-powered fraud detection, and other technologies, which can help institutions identify and prevent fraudulent transactions in real-time, even during the holiday surge.
- **Offer security tools:** Financial institutions should encourage accountholders to use multifactor authentication, personal account alerts, and other account protection tools.
- **Increase monitoring:** Financial institutions should increase monitoring of transactions during the holiday season to detect unusual or suspicious activity.

RISK MITIGATION RESOURCES

- [Sign up](#) for our **Let's Talk Fraud** quarterly webinars
- [View](#) additional risk resources

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The image contains two side-by-side promotional banners. The left banner is titled "Allied Insights" and features a red button with a white double arrow icon and the text "LEARN MORE". Below the button, it says "Forward-thinking content and original insights into the markets you serve, to help you grow, protect and evolve your business." The right banner is titled "Stay Informed" and features an orange button with a white double arrow icon and the text "SUBSCRIBE". Below the button, it says "Sign-up for our newsletters to receive expert education and insights on top-of-mind industry topics and receive resources coming to your inbox." Both banners have a blue background with a subtle globe pattern.



LinkedIn

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.